

#2

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Tomihiko AZUMA **Docket:** 14717
Serial No: Unassigned **Dated:** June 26, 2001
Filed: Herewith
For: SINGLE SIGN-ON SYSTEM AND
AND SINGLE SIGN-ON METHOD
FOR A WEB SITE AND RECORDING
SYSTEM



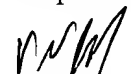
Assistant Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231

CLAIM OF PRIORITY

Sir:

Applicant in the above-identified application hereby claims the right of priority in connection with Title 35 U.S.C. §119 and in support thereof, herewith submits a certified copy of Japanese Patent Application 2000-214625, filed on July 14, 2000.

Respectfully submitted,


Paul J. Esatto, Jr.
Registration No. 30,749

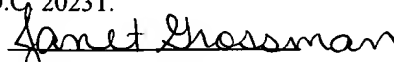
Scully, Scott, Murphy & Presser
400 Garden City Plaza
Garden City, NY 11530
(516) 742-4343
PJE:ahs

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Mailing Label Number: EL915257625US
Date of Deposit: June 26, 2001

I hereby certify that this correspondence is being deposited with the United States Postal Service Express Mail Post Office to Addressee service under 37 C.F.R. §1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Dated: June 26, 2001


Janet Grossman

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JP821 U.S. PRO
09/891992
06/26/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年 7月14日

出 願 番 号
Application Number:

特願2000-214625

出 願 人
Applicant(s):

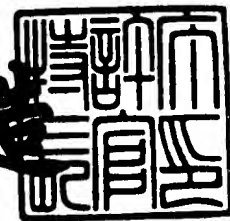
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月25日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3043804

【書類名】 特許願

【整理番号】 60301692

【提出日】 平成12年 7月14日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00
G06F 13/00
H04L 12/28
H04L 12/58

【発明者】

【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

【氏名】 東 富彦

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100080816

【弁理士】

【氏名又は名称】 加藤 朝道

【電話番号】 045-476-1131

【手数料の表示】

【予納台帳番号】 030362

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9304371

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 W e b サイトに対するシングルサインオンシステム及び方法並びに記録媒体

【特許請求の範囲】

【請求項 1】

インターネットを介してW e b サーバにアクセスするユーザ端末と、前記W e b サーバとの間に、W e b サイトにおけるユーザ認証を代行するユーザ認証プロキシ装置を備え、

前記ユーザ認証プロキシ装置は、ユーザ認証を代行するために必要なデータを記録する手段を備え、

ユーザ端末で指定したW e b サイトに対するユーザ認証を前記ユーザ認証プロキシ装置に代行させ、前記ユーザ端末におけるユーザ認証のための操作を削減する、ことを特徴とする、W e b サイトに対するシングルサインオンシステム。

【請求項 2】

前記ユーザ認証プロキシ装置は、ユーザ認証時に前記ユーザ端末と前記W e b サーバとの間で送受信されるデータを記憶手段に保存し、ユーザ認証の代行時、前記記憶手段に記憶されているデータを再利用する、ことを特徴とする、請求項 1 記載のW e b サイトに対するシングルサインオンシステム。

【請求項 3】

インターネットを介してW e b サーバにアクセスするユーザ端末と、前記W e b サーバとの間にユーザ認証プロキシ装置を備え、

前記ユーザ認証プロキシ装置は、ユーザがユーザ端末を利用してインターネットを介して前記W e b サーバとの間で行った一連のユーザ認証プロセスに係わる情報として、W e b サイトのURL (U n i f o r m R e s o u c e L o c a t o r) 、ユーザ認証用に前記ユーザ端末が前記W e b サーバから受信したデータ、ユーザ認証用に前記ユーザ端末がW e b サーバへ送信したユーザ認証用データの 3 つのデータを組として記憶手段に保存する手段と、

前記ユーザが任意のユーザ端末を利用して前記W e b サイトのURL を指定した場合、前記URL で指示されているW e b サーバに接続要求を送信し、前記W

e bサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する手段と、

を備えた、ことを特徴とするWebサイトに対するシングルサインオンシステム。

【請求項4】

インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に配設されるユーザ認証プロキシ装置が、

ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する手段と、

前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する手段と、

を備えた、ことを特徴とするユーザ認証プロキシ装置。

【請求項5】

インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に配設されるユーザ認証プロキシ装置が、

前記ユーザ認証プロキシ装置を利用するユーザが正当な利用者であることを確認するために必要な情報として、利用者を一意に識別するユーザ識別子とパスワ

ードを記憶するプロキシ利用者認証用データ記憶部と、

利用者を一意に識別するユーザ識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末がWebサーバから受信した受信データと、ユーザ認証用に前記ユーザ端末が前記Webサーバに送信した送信データとの組を記憶するWebサイト利用者認証用データ記憶部と、を備えた記憶装置と、

前記プロキシ利用者認証用データ記憶部に保存されているデータを利用して、ユーザがユーザ認証プロキシ装置の正当な利用者であるかどうかの認証を行うプロキシ利用者認証手段と、

ユーザが前記ユーザ認証プロキシ装置にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するためのユーザ識別子と組にして前記Webサイト利用者認証用データ記憶部に保存するURL保存手段と、

ユーザ認証を行うために前記ユーザ端末が前記Webサーバから受信したデータを、前記Webサイト利用者認証用データ記憶部に保存する受信データ保存手段と、

ユーザ認証を行うために前記ユーザ端末が前記Webサーバへ送信したデータを、前記Webサイト利用者認証用データ記憶部に保存する送信データ保存手段と、

前記ユーザがユーザ端末で指定したURLと、前記Webサイト利用者認証用データ記憶部に保存されているURLとを比較し、前記ユーザ認証プロキシ装置がユーザ認証を代行するURLであるか否かを判断するURL比較手段と、

前記ユーザが指定したURLを使用して前記Webサーバに接続し、前記Webサーバから受信したデータと、前記Webサイト利用者認証用データ記憶部に保存されている受信データとを比較する受信データ比較手段と、

前記ユーザ識別子、URL、および前記Webサーバから受信した受信データの組が、前記Webサイト利用者認証用データ記憶部に存在する場合には、ユーザ認証の代行が可能であるものと判定し、ユーザ認証を代行するために、前記Webサイト利用者認証用データ記憶部から対応する送信データを取得して前記Webサーバへ送信する代行認証用データ送信手段と、

を備えたことを特徴とするユーザ認証プロキシ装置。

【請求項6】

インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に、Webサイトにおけるユーザ認証を代行するユーザ認証プロキシ装置を配置し、

前記ユーザ認証プロキシ装置は、ユーザ認証を代行するために必要なデータを記録し、

ユーザ端末の種類を問わず、ユーザがURLで指定したWebサイトに対するユーザ認証を、前記ユーザ認証プロキシ装置に代行させるようにしたことを特徴とするWebサイトに対するユーザ認証代行方法。

【請求項7】

前記ユーザ認証プロキシ装置は、ユーザ認証時に前記ユーザ端末と前記Webサーバとの間で送受信されるデータを保存し、ユーザ認証の代行時、前記保存されているデータを再利用する、ことを特徴とする、請求項6記載のWebサイトに対するユーザ認証代行方法。

【請求項8】

インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間にユーザ認証プロキシを設け、

ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存するステップと、

前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信するステップと、

前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せ

ず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信するステップと、

を含む、ことを特徴とするWebサイトに対するユーザ認証代行方法。

【請求項 9】

インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に配設されるユーザ認証プロキシ装置が、

(a) ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する処理と、

(b) 前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する処理と、

の前記(a)及び(b)の処理を、前記ユーザ認証プロキシ装置を構成するコンピュータに実行させるためのプログラムを記録した記録媒体。

【請求項 10】

インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間に配設されるユーザ認証プロキシ装置が、

前記ユーザ認証プロキシ装置を利用するユーザが正当な利用者であることを確認するために必要な情報として、利用者を一意に識別するユーザ識別子とパスワードを記憶するプロキシ利用者認証用データ記憶部と、

利用者を一意に識別するユーザ識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末がWebサーバから受信した受信データと、ユーザ認証用に前

記ユーザ端末が前記W e bサーバに送信した送信データとの組を記憶するW e bサイト利用者認証用データ記憶部と、を備え、

(a) 前記プロキシ利用者認証用データ記憶部に保存されているデータを利用して、ユーザがユーザ認証プロキシ装置の正当な利用者であるかどうかの認証を行うプロキシ利用者認証処理と、

(b) ユーザが前記ユーザ認証プロキシ装置にユーザ認証を代行させるように指示したW e bサイトのU R Lを、ユーザを一意に識別するための識別子と組にして前記W e bサイト利用者認証用データ記憶部に保存するU R L保存処理と、

(c) ユーザ認証を行うために前記ユーザ端末が前記W e bサーバから受信したデータを、前記W e bサイト利用者認証用データ記憶部に保存する受信データ保存処理と、

(d) ユーザ認証を行うために前記ユーザ端末が前記W e bサーバへ送信したデータを、前記W e bサイト利用者認証用データ記憶部に保存する送信データ保存処理と、

(e) 前記ユーザがユーザ端末で指定したU R Lと、前記W e bサイト利用者認証用データ記憶部に保存されているU R Lとを比較し、前記ユーザ認証プロキシ装置がユーザ認証を代行するU R Lであるかどうかを判断するU R L比較処理と、

(f) 前記ユーザが指定したU R Lを使用して前記W e bサーバに接続し前記W e bサーバから受信したデータと、前記W e bサイト利用者認証用データ記憶部22に保存されている受信データとを比較する受信データ比較処理と、

(g) 前記ユーザ識別子、U R L、および前記W e bサーバから受信した受信データの組が、W e bサイト利用者認証用データ記憶部に存在する場合には、代行認証が可能と判定し、ユーザ認証を代行するための送信データを前記W e bサイト利用者認証用データ記憶部から取得し、前記W e bサーバへ送信する代行認証用データ送信処理と、

の前記(a)乃至(g)の処理を、前記ユーザ認証プロキシ装置を構成するコンピュータに実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、WWW (W o l r d W i d e W e b) サーバの認証の代行システムに関し、特に、任意のW e b サイトに対するシングルサインオンシステムに関する。

【 0 0 0 2 】

【従来の技術】

ユーザ認証を必要とするW e b サイトが増加するに従って、ユーザ認証を行うために必要な操作が増加し、ユーザに負担がかかるようになってきた。

【 0 0 0 3 】

さらに、ユーザは、複数のユーザIDやパスワードを覚えることは、負担となり、また、困難であることから、シングルサインオンシステムが求められている。

【 0 0 0 4 】

これに対して、特定のW e b サイトだけを対象とする形でのシングルサインオンシステムや、PKI (P u b l i c K e y I n f r a s t r u c t u r e ; 公開鍵インフラストラクチャ) を利用した標準的な方法が利用され始めている。

【 0 0 0 5 】

なお、例えば特開 2 0 0 0 - 3 3 3 4 号公報には、ユーザからの要求をゲートウェイで受信して該当する他の情報提供サーバあるいは他のゲートウェイにユーザID/パスワードを変換して送信し、その応答を受信したとき逆変換して要求元に送信し、ユーザからみて1つのユーザIDとパスワードで所望の情報サービスを提供するゲートウェイシステムが提案されている。

【 0 0 0 6 】

【発明が解決しようとする課題】

しかしながら、この従来のシステムには、次のような問題点がある。

【 0 0 0 7 】

特定のW e b サイトだけを対象とするシステムでは、任意のW e b サイトをそ

のままの形で、シングルサインオンシステムに加えることはできない。

【0008】

そして、Webサイトのユーザ認証方法を変更するか、特定の場所にWebサイトを配置するなどの対処が必要となる場合が多い。

【0009】

一方、PKIをベースにしたユーザ認証方法を利用するためには、ユーザ端末側に、セキュリティ機能を具備することが必要とされる。

【0010】

近時、Webサイトを利用するユーザ端末が、従来のPC（パーソナルコンピュータ）から、携帯電話や携帯情報端末、FAX（ファクシミリ装置）などの端末へ広がるとともに、セキュリティ機能を持たない端末が増加し、すべての端末がPKIに対応することは、事実上、不可能になっている。

【0011】

したがって、本発明は、上記問題点に鑑みてなされたものであって、その目的は、ユーザ認証を必要とする任意のWebサイトに対して、ユーザ認証を代行することで、ユーザの負担を軽減するシステム及び方法並びに記録媒体を提供することにある。

【0012】

【課題を解決するための手段】

前記目的を達成する本発明は、インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に、Webサイトにおけるユーザ認証を代行するユーザ認証プロキシを配置し、ユーザ端末の種類を問わず、ユーザがURLで指定したWebサイトに対するユーザ認証を、前記ユーザ認証プロキシに代行させるようにしたものである。

【0013】

本発明は、インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間にユーザ認証プロキシ装置を備え、前記ユーザ認証プロキシ装置は、ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、Webサイト

のURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する手段と、前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する手段とを備えている。

【0014】

【発明の実施の形態】

本発明は、ユーザ認証が必要な複数のWebサイトを、ユーザ端末から利用するシステムにおいて、Webサーバと、ユーザ端末との間にWebサイトにおけるユーザ認証を代行するプロキシを置き、このプロキシに、Webサイトにおけるユーザ認証を代行させることにより、Webサイトを利用する際に、ユーザがユーザ端末で実行しなければならないユーザ認証作業の操作回数を、大幅に削減するものである。

【0015】

本発明は、その好ましい一実施の形態において、図1を参照すると、ユーザ認証プロキシ(2)は、ユーザ認証を代行するために必要なデータを記録する。

【0016】

ユーザ認証プロキシ(2)は、ユーザがユーザ端末(1)を利用してインターネット(3)を介してWebサーバ(4)との間で行った一連のユーザ認証プロセスに係わる情報を保存する。

【0017】

保存するデータとしては、好ましくは、

・WebサイトのURL (Uniform Resource Locator

）、

- ・ ユーザ認証用にユーザ端末（１）がWebサーバ（４）から受信したデータ
- ・ ユーザ認証用にユーザ端末（１）がWebサーバ（４）へ送信したデータよりなる。

【 0 0 1 8 】

これら３つのデータの組を保存することにより、ユーザ端末（１）の種類を問わず、ユーザがURLで指定したWebサイトに対するユーザ認証を、ユーザ認証プロキシ（２）に代行させることができる。

【 0 0 1 9 】

ユーザが任意のユーザ端末（１）を利用してWebサイトのURLを指定した場合、ユーザ認証プロキシ（２）は、URLで指示されているWebサーバ（４）に接続要求を送信し、Webサーバ（４）から該URLに対するデータを受信する。

【 0 0 2 0 】

ユーザ認証プロキシ（２）は、この受信データと、あらかじめ保存してある受信データとを比較し、両者が等しい場合には、Webサーバ（４）からの受信データをユーザ端末（１）に転送せず、あらかじめ保存されているユーザ認証用の送信データを、ユーザに代わってWebサーバ（４）に返却する。

【 0 0 2 1 】

本発明は、その好ましい一実施の形態において、インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間に設けられたユーザ認証プロキシにおいて、（a）ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL（Uniform Resource Locator）、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの３つのデータを組として記憶手段に保存する処理と、

（b）前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを

指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する処理と、

の前記(a)、(b)の処理は、ユーザ認証プロキシのデータ処理装置(コンピュータ)で実行されるプログラムにより実現され、該プログラムを記録した記録媒体(磁気ディスク、磁気テープ、光ディスク、もしくは半導体メモリ等)から該プログラムをデータ処理装置に読み出して実行することで、ユーザ認証プロキシを実施することができる。

【0022】

より詳細には、本発明は、その好ましい一実施の形態において、インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間に設けられたユーザ認証プロキシ装置において、前記ユーザ認証プロキシ装置を利用するユーザが正当な利用者であることを確認するために必要な情報として、利用者を一意に識別するユーザ識別子とパスワードを記憶するプロキシ利用者認証用データ記憶部(221)と、利用者を一意に識別するユーザ識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末がWebサーバから受信した受信データと、ユーザ認証用に前記ユーザ端末が前記Webサーバに送信した送信データとの組を記憶するWebサイト利用者認証用データ記憶部(222)と、を備えた記憶装置(22)と、前記プロキシ利用者認証用データ記憶部(221)に保存されているデータを利用して、ユーザが当該ユーザ認証プロキシ装置の正当な利用者であるかどうかの認証を行うプロキシ利用者認証手段(211)と、ユーザが前記ユーザ認証プロキシ装置にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するためのユーザ識別子と組にして前記Webサイト利用者認証用データ記憶部に保存するURL保存手段(212)と、ユーザ認証を行うために前記ユーザ端末が前記Webサーバから受信したデータを、前記Webサイト利用者認証用データ記憶部に保存する受信データ保存

手段（213）と、ユーザ認証を行うために前記ユーザ端末が前記Webサーバへ送信したデータを、前記Webサイト利用者認証用データ記憶部（222）に保存する送信データ保存手段（214）と、前記ユーザがユーザ端末で指定したURLと、前記Webサイト利用者認証用データ記憶部（222）に保存されているURLとを比較し、前記ユーザ認証プロキシ装置がユーザ認証を代行するURLであるかどうかを判断するURL比較手段（215）と、前記ユーザが指定したURLを使用して前記Webサーバに接続し、前記Webサーバから受信したデータと、前記Webサイト利用者認証用データ記憶部に保存されている受信データとを比較する受信データ比較手段（216）と、前記ユーザ識別子、URL、および前記Webサーバから受信した受信データの組が、前記Webサイト利用者認証用データ記憶部に存在する場合には、代行認証が可能であると判定し、ユーザ認証を代行するための、対応する送信データを前記Webサイト利用者認証用データ記憶部から取得し、前記Webサーバへ送信する代行認証用データ送信手段（217）と、を備える。ユーザ認証プロキシ装置における上記各手段は、ユーザ認証プロキシのデータ処理装置（コンピュータ）で実行されるプログラムにより、その処理・機能が実現され、該プログラムを記録した記録媒体（磁気ディスク、磁気テープ、光ディスク、もしくは半導体メモリ等）から該プログラムをデータ処理装置に読み出して実行することで、ユーザ認証プロキシ装置を実施することができる。

【0023】

【実施例】

上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して以下に説明する。図1は、本発明の一実施例のシステム構成を示す図である。

【0024】

図1を参照すると、本発明の一実施例は、有線あるいは無線によりインターネット3と相互に接続できる機能を有するパーソナルコンピュータ、携帯電話機、携帯情報端末、FAXなどのユーザ端末1と、インターネット3上でユーザ認証が必要なWebサイトを提供している情報処理装置であるWebサーバ4と、ユ

ーザ端末1とインターネット3との接続を仲介する情報処理装置であるユーザ認証プロキシ2とを含む。

【0025】

図2は、本発明の一実施例におけるユーザ認証プロキシ2の構成の一例を示す図である。図2を参照すると、ユーザ認証プロキシ2は、プログラム制御により動作するデータ処理装置21と、情報を記憶する記憶装置22と、を含む。

【0026】

記憶装置22は、プロキシ利用者認証用データ記憶部221と、Webサイト利用者認証用データ記憶部222と、を備えている。

【0027】

プロキシ利用者認証用データ記憶部221には、ユーザ認証プロキシ2を利用する利用者が正当な利用者であることを確認するために必要な情報が記憶されている。

【0028】

利用者は、Webサイトのユーザ認証を、ユーザ認証プロキシ2に代行させる前に、利用者自身が正当な利用者であることをユーザ認証プロキシ2に証明しなければならない。

【0029】

Webサイト利用者認証用データ記憶部222には、利用者を一意に識別する識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末1がWebサーバ4から受信したデータと、ユーザ認証用にユーザ端末1がWebサーバ4に送信したデータとの組が記憶されている。

【0030】

データ処理装置21は、プロキシ利用者認証手段211と、URL保存手段212と、受信データ保存手段213と、送信データ保存手段214と、URL比較手段215と、受信データ比較手段216と、代行認証用データ送信手段217とを備えている。

【0031】

プロキシ利用者認証手段211は、プロキシ利用者認証用データ記憶部221

に保存されているデータを利用して、ユーザがユーザ認証プロキシ2の正当な利用者であるかどうかの認証を行う。

【0032】

URL保存手段212は、ユーザがユーザ認証プロキシ2にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するための識別子と組にしてWebサイト利用者認証用データ記憶部222に保存する。

【0033】

受信データ保存手段213は、ユーザ認証を行うためにユーザ端末1がWebサーバ4から受信したデータを、Webサイト利用者認証用データ記憶部222に保存する。

【0034】

送信データ保存手段214は、ユーザ認証を行うためにユーザ端末1がWebサーバ4へ送信したデータを、Webサイト利用者認証用データ記憶部222に保存する。

【0035】

URL比較手段215は、ユーザがユーザ端末1で指定したURLと、Webサイト利用者認証用データ記憶部222に保存されているURLとを比較し、ユーザ認証プロキシ2がユーザ認証を代行するURLであるかどうかを判断する。

【0036】

受信データ比較手段216は、ユーザが指定したURLを使用して、その時点で実際にWebサーバ4に接続してWebサーバ4から受信したデータと、Webサイト利用者認証用データ記憶部222に保存されている受信データとを比較する。

【0037】

代行認証用データ送信手段217は、ユーザ認証を代行するための送信データを、Webサイト利用者認証用データ記憶部222から取得し、Webサーバ4へ送信する。

【0038】

本発明の一実施例におけるデータ処理装置21の上記各手段211～217は

、データ処理装置 2 1 で実行されるプログラムによりその処理・機能が実現される。

【 0 0 3 9 】

次に図 1 乃至図 8 を参照して、本発明の一実施例の動作について詳細に説明する。

【 0 0 4 0 】

まず、ユーザがユーザ認証を代行させるためのデータをユーザ認証プロキシ 2 に保存する動作について、図 3 に示した流れ図を参照して、詳細に説明する。

【 0 0 4 1 】

ユーザは、ユーザ端末 1 を利用して、ユーザ認証代行に必要なデータの保存開始要求を、ユーザ認証プロキシ 2 に送信する（ステップ A 1）。

【 0 0 4 2 】

ユーザ認証プロキシ 2 のプロキシ利用者認証手段 2 1 1 は、ユーザがユーザ認証プロキシ 2 の正当なユーザであることを確認するために必要な認証用データを要求する（ステップ A 2）。

【 0 0 4 3 】

ユーザは、ユーザ端末 1 から、ユーザ認証プロキシ 2 の正当なユーザであることを示すデータを送信する（ステップ A 3）。

【 0 0 4 4 】

ユーザ認証プロキシ 2 のプロキシ利用者認証手段 2 1 1 は、ユーザ端末 1 から送信されたデータと、プロキシ利用者認証用データ記憶部 2 2 1 に保存されているデータとを比較して、当該ユーザが正当なユーザであるが否かを判定する（ステップ A 4）。

【 0 0 4 5 】

正当なユーザであると判定されなかった場合には、ユーザ認証プロキシ 2 は代行認証用データの保存開始要求を拒否する（ステップ A 5）。

【 0 0 4 6 】

一方、ステップ A 4 において、正当なユーザであると判定された場合には、ユーザ認証プロキシ 2 は、代行認証用データの保存開始を許可する（ステップ A 6

）。

【 0 0 4 7 】

図 5 は、プロキシ利用者認証用データ記憶部 2 2 1 に記憶されているデータの一例を示す図である。図 5 に示す例では、ユーザ認証プロキシ 2 のユーザを認証するデータとして、ユーザを一意に識別するためのユーザ ID と、パスワードが用いられている。

【 0 0 4 8 】

ユーザがユーザ ID として、“0 0 0 0 1”を指定し、パスワードとして、“p K i # 1 _ *)”を指定した場合には、正当なユーザと認証され、それ以外のパスワードが指定された場合には、正当なユーザであるとは認証されない。

【 0 0 4 9 】

ユーザ認証プロキシ 2 の正当なユーザであると認証されたユーザは、ユーザ端末 1 から、Web サイトのユーザ認証用 URL (u n i f o r m r e s o u c e l o c a t o r) を、ユーザ認証プロキシ 2 に送信する (ステップ A 7) 。

【 0 0 5 0 】

ユーザ認証プロキシ 2 は、ユーザ端末 1 から送信された URL を受け取り、URL をユーザを一意に識別するための識別子と組にして、一時記憶に記憶した上で、Web サーバ 4 に接続する (ステップ A 8) 。

【 0 0 5 1 】

Web サーバ 4 は、ユーザ認証プロキシ 2 から URL を受信し、URL に対するデータを、ユーザ認証プロキシ 2 へ返信する (ステップ A 9) 。

【 0 0 5 2 】

ユーザ認証プロキシ 2 は、Web サーバ 4 から受信したデータを、ユーザを一意に識別するための識別子および URL と組にして一時記憶に記憶した上で、ユーザ端末 1 へデータを送信する (ステップ A 1 0) 。

【 0 0 5 3 】

ユーザはユーザ端末 1 から、Web サイトのユーザ認証に必要なデータを、ユーザ認証プロキシ 2 へ送信する (ステップ A 1 1) 。

【 0 0 5 4 】

ユーザ認証プロキシ2は、ユーザ端末1から送信されたWebサイトのユーザ認証用データを受け取り、これを、ユーザを一意に識別するための識別子およびURLと組にして一時記憶に記憶した上で、Webサーバ4へ送信する（ステップA12）。

【0055】

Webサーバ4は、ユーザ認証プロキシ2から送信されたユーザ認証用データを検査し、Webサイトの正当なユーザであるか否かを判定する（ステップA13）。

【0056】

Webサーバ4が、ユーザをWebサイトの正当なユーザではないと判定した場合には、ユーザ認証に失敗したことを、ユーザ認証プロキシ2を通して、ユーザ端末1に通知する（ステップA14）。

【0057】

Webサーバ4が、ユーザをWebサイトの正当なユーザであると判定した場合には、ユーザ認証に成功したことを、ユーザ認証プロキシ2を通してユーザ端末1に通知する（ステップA15）。

【0058】

Webサイトのユーザ認証に成功した場合、ユーザは、ユーザ端末1を利用して、代行認証用データの保存終了を、ユーザ認証プロキシ2へ送信する（ステップA16）。

【0059】

ユーザ認証プロキシ2は、URL保存手段212、受信データ保存手段213、送信データ保存手段214を利用して、一時記憶に記憶されている、

- ・ユーザ識別子、

- ・URL、

- ・ユーザ端末1がWebサーバ4から受信したデータ、および、

- ・ユーザ端末1がWebサーバ4へ送信したデータ

を、Webサイト利用者認証用データ記憶部222へ保存する（ステップA17）。

【 0 0 6 0 】

図 6 は、Web サイト利用者認証用データ記憶部 2 2 2 に記憶されているデータの一例を示す図である。図 6 に示す例では、

- ・ ユーザを一意に識別するためのユーザ ID、
- ・ URL、
- ・ Web サーバからの受信データ、および、
- ・ Web サーバからの送信データ

の組が保存されている。

【 0 0 6 1 】

ユーザ ID が “ 0 0 0 0 1 ” のユーザに対しては、“http://www.nec.co.jp/customer.html” の URL に対する送受信データと、“http://www.shop1.co.jp/buyer.html” の URL に対する送受信データが保存されており、これら 2 つの URL で示される Web サイトのユーザ認証をユーザ認証プロキシ 2 が代行できるように設定されている。

【 0 0 6 2 】

同様に、ユーザ ID が “ 0 0 0 0 2 ” のユーザに対しては、“http://www.nec.co.jp/customer.html” の URL に対する送受信データと、“http://www.books.co.jp/buyer.html” の URL に対する送受信データが保存されており、これら 2 つの URL で示される Web サイトのユーザ認証をユーザ認証プロキシ 2 が代行できるように設定されている。

【 0 0 6 3 】

図 7 は、図 6 における受信データ 1 および送信データ 1 の例を示す図である。Web サーバ 4 からの受信データ 1 として、HTML (HyperText Markup Language) のテキストが保存されている。この HTML テキストにおいて、<FORM ACTION...> は、CGI (/cgi-bin) にデータを入力するためのタグであり、<table> タグにおいて、UserID 欄、Password 欄の表示と、入力 (入力フォームは <input> で規定される)、及び、value = “Submit” で規定される Submit ボタンが表示され、Submit ボタンの押下により、入力データが CGI に受け渡され

る。Webサーバ4へ送信する送信データ1としては、CGI (Common Gateway Interface) のPOSTメソッドで引き渡すテキスト (uid (ユーザ識別子) が00001でpwdがn#ilce_9) が保存されている。

【0064】

図8は、図6における受信データ2および送信データ2の例を示す図である。図8に示す例では、Webサーバから受信したデータとして、XML (eXtensible Markup Language) のテキスト (<?xml:stylesheetで始まる行は、このXML文書を表示すべきXLT (eXtensible Stylesheet Language) スクリプトが"member.xsl"であることを示す) が保存されており、Webサーバへ送信するデータとしても、XMLのテキストが保存されている。

【0065】

次に、ユーザがユーザ認証プロキシ2を利用して、Webサイトのユーザ認証を代行させる動作を、図4の流れ図を参照して詳細に説明する。

【0066】

ユーザは、ユーザ端末1から、ユーザ認証プロキシ2の使用を要求する (ステップB1)。

【0067】

ユーザ認証プロキシ2において、プロキシ利用者認証手段211が、ユーザがユーザ認証プロキシ2の正当なユーザであることを確認するために必要な認証用データを要求する (ステップB2)。

【0068】

ユーザは、ユーザ端末1から、ユーザ認証プロキシ2の正当なユーザであることを示すデータを送信する (ステップB3)。

【0069】

ユーザ認証プロキシ2のプロキシ利用者認証手段211は、ユーザ端末1から受信したデータと、プロキシ利用者認証用データ記憶部221に保存されているデータとにより、ユーザが正当なユーザが否かを判定する (ステップB4)。

【 0 0 7 0 】

正当なユーザであると判定されなかった場合には、ユーザ認証プロキシ 2 はユーザの利用を拒否する（ステップ B 5）。

【 0 0 7 1 】

ステップ B 4 において、正当なユーザであると判定された場合には、ユーザ認証プロキシ 2 はユーザの利用を許可する（ステップ B 6）。

【 0 0 7 2 】

図 5 は、プロキシ利用者認証用データ記憶部 2 2 1 に記憶されているデータの一例を示す図である。図 5 に示す例では、ユーザ認証プロキシ 2 のユーザを認証するデータとして、ユーザを一意に識別するためのユーザ ID と、パスワードが用いられている。ユーザがユーザ ID として “0 0 0 0 1” を指定し、パスワードとして “p K i # 1 _ * ” を指定した場合には正当なユーザと認証され、それ以外のパスワードが指定された場合には正当なユーザであるとは認証されない。

【 0 0 7 3 】

ユーザ認証プロキシ 2 の正当なユーザであると認証されたユーザは、ユーザ端末 1 を利用して Web サイトのユーザ認証用 URL をユーザ認証プロキシ 2 に送信する（ステップ B 7）。

【 0 0 7 4 】

ユーザ認証プロキシ 2 は、ユーザ端末 1 から受信した URL を、ユーザを一意に識別するための識別子と組にして一時記憶に記憶した上で、Web サーバ 4 に接続する（ステップ B 8）。

【 0 0 7 5 】

Web サーバ 4 は、ユーザ認証プロキシ 2 から URL を受信し、URL に対するデータをユーザ認証プロキシ 2 へ返信する（ステップ B 9）。

【 0 0 7 6 】

ユーザ認証プロキシ 2 は、Web サーバ 4 から受信したデータを、ユーザを一意に識別するための識別子および URL と組にして一時記憶に記憶する（ステップ B 1 0）。

【 0 0 7 7 】

ユーザ認証プロキシ 2 は、URL 比較手段 2 1 5 および受信データ比較手段 2 1 6 を利用して、一時記憶に記憶されているユーザ識別子、URL、および Web サーバから受信した受信データの組が、Web サイト利用者認証用データ記憶部 2 2 2 に存在するか否かをチェックし、代行認証が可能か否かを判定する（ステップ B 1 1）。

【 0 0 7 8 】

一時記憶に記憶されているユーザ識別子、URL、および Web サーバから受信した受信データの組が、Web サイト利用者認証用データ記憶部 2 2 2 に存在しない場合には、代行認証が不可能と判定し、Web サーバ 4 から受信したデータをそのままユーザ端末 1 へ返信する（ステップ B 1 2）。

【 0 0 7 9 】

一時記憶に記憶されているユーザ識別子、URL、および Web サーバから受信した受信データの組が、Web サイト利用者認証用データ記憶部 2 2 2 に存在する場合には、代行認証が可能と判定し、代行認証用データ送信手段 2 1 7 を利用して、対応する送信データを Web サイト利用者認証用データ記憶部 2 2 2 から取得し、Web サーバ 4 へ送信する（ステップ B 1 3）。

【 0 0 8 0 】

図 6 および図 7 の例では、ユーザ ID が “0 0 0 0 1” のユーザが、“http://www.nec.co.jp/customer.html” の URL にアクセスした場合に、Web サーバが図 7 における受信データ 1 と同じテキストをユーザ認証プロキシ 2 に返却すると、ユーザ認証プロキシ 2 は、代行認証が可能と判定し、図 7 の送信データ 1 を Web サーバ 4 へ送信する。

【 0 0 8 1 】

図 6 および図 8 の例では、ユーザ ID が “0 0 0 0 1” のユーザが、“http://www.shop1.co.jp/buyer.html” の URL にアクセスした場合に、Web サーバが図 8 における受信データ 2 と同じテキストをユーザ認証プロキシ 2 に返却すると、ユーザ認証プロキシ 2 は代行認証が可能と判定し、図 8 の送信データ 2 を Web サーバ 4 へ送信する。

【0082】

【発明の効果】

以上説明したように本発明によれば下記記載の効果を奏する。

【0083】

本発明の第1の効果は、ユーザ端末とWebサーバ間に、ユーザ認証を代行するプロキシを配置したことにより、ユーザ認証を必要とする任意のWebサイトに対して、シングルサインオン (single sign on) によりユーザ認証を行うことができる、ということである。

【0084】

前述したように、ユーザ認証を必要とするWebサイトは急速に増加しているが、ユーザを認証する方法は統一されていず、Webサイト毎に個別の方法を採用している場合が多いというのが現状であり、本発明によれば、このような個別のユーザ認証方法を採用しているWebサイトに対して、Webサイト提供者に何ら負担をかけることなく、シングルサインオンにより、ユーザ認証可能としており、本発明の有効性は顕著である。

【0085】

また、本発明の第2の効果は、携帯電話や携帯情報端末をユーザ端末とするシステムにおいては、シングルサインオンによって必要なすべてのWebサイトにアクセス可能となり、ユーザ認証に必要な操作を大幅に削減し、ユーザの負担を軽減し、操作性、利便性を向上させる、ということである。

【0086】

その理由は、本発明においては、ユーザ端末とWebサーバとの間にユーザ認証を行うプロキシを置き、ユーザ認証時にユーザ端末とWebサーバとの間で送受信されるデータを、そのままの形でプロキシに保存し、再利用しているためである。そして、Webサイトごとにユーザ認証の方法が異なる場合でも、実際にネットワークを流れるデータをそのままの形で保存しておくことで、ユーザ認証に再利用することができる、ためである。

【図面の簡単な説明】

【図1】

本発明の一実施例の構成を示す図である。

【図 2】

本発明の一実施例におけるユーザ認証プロキシの構成を示す図である。

【図 3】

本発明の一実施例の動作を説明するための流れ図である。

【図 4】

本発明の一実施例の動作を説明するための流れ図である。

【図 5】

本発明の一実施例におけるプロキシ利用者認証用データ記憶部の内容の一例を示す図である。

【図 6】

本発明の一実施例におけるWebサイト利用者認証用データ記憶部の内容の一例を示す図である。

【図 7】

本発明の一実施例における受信データと送信データの一例を示す図である。

【図 8】

本発明の一実施例における受信データと送信データの一例を示す図である。

【符号の説明】

- 1 ユーザ端末
- 2 ユーザ認証プロキシ
- 3 インターネット
- 4 Webサーバ
- 21 データ処理装置
- 211 プロキシ利用者認証手段
- 212 URL保存手段
- 213 受信データ保存手段
- 214 送信データ保存手段
- 215 URL比較手段
- 216 受信データ比較手段

217 代行認証用データ送信手段

22 記憶装置

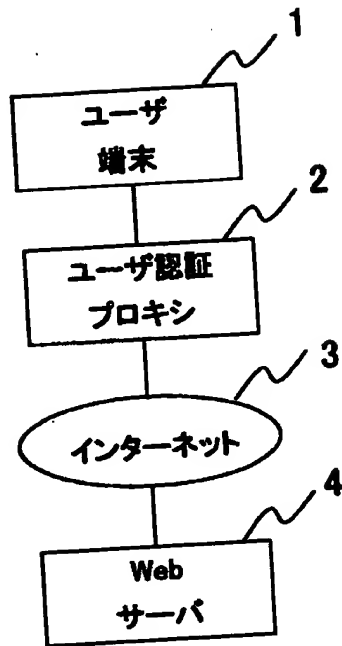
221 プロキシ利用者認証用データ記憶部

222 Webサイト利用者認証用データ記憶部

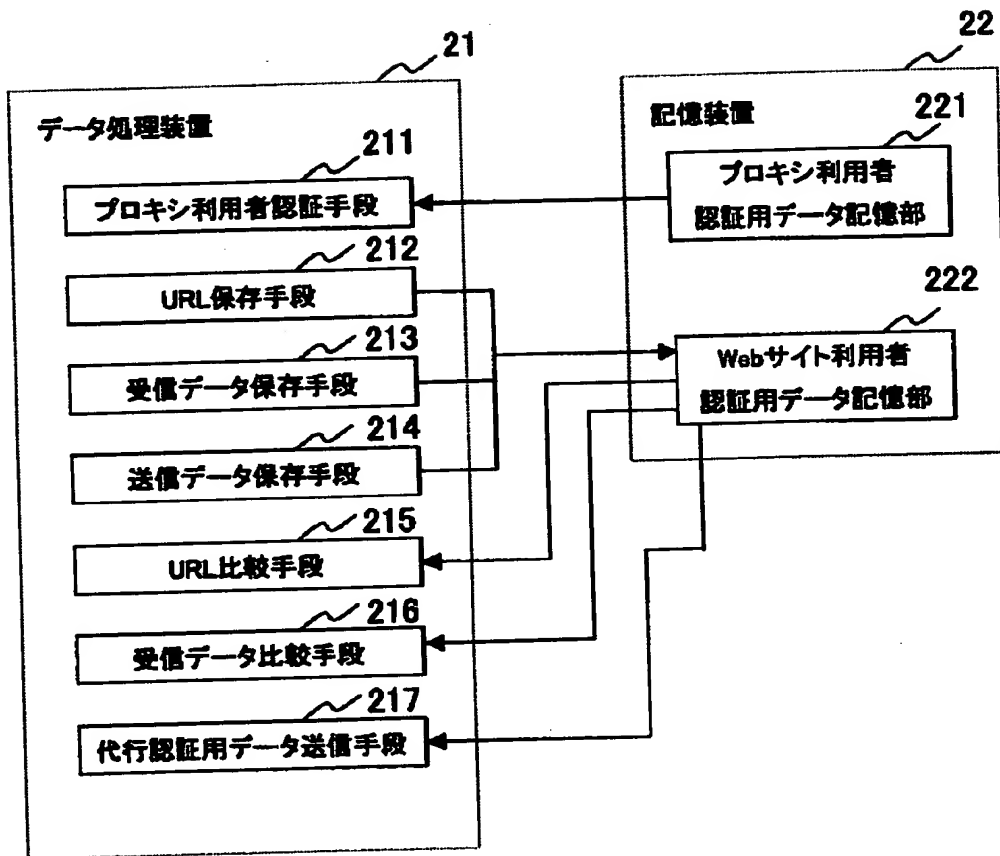
【書類名】

図面

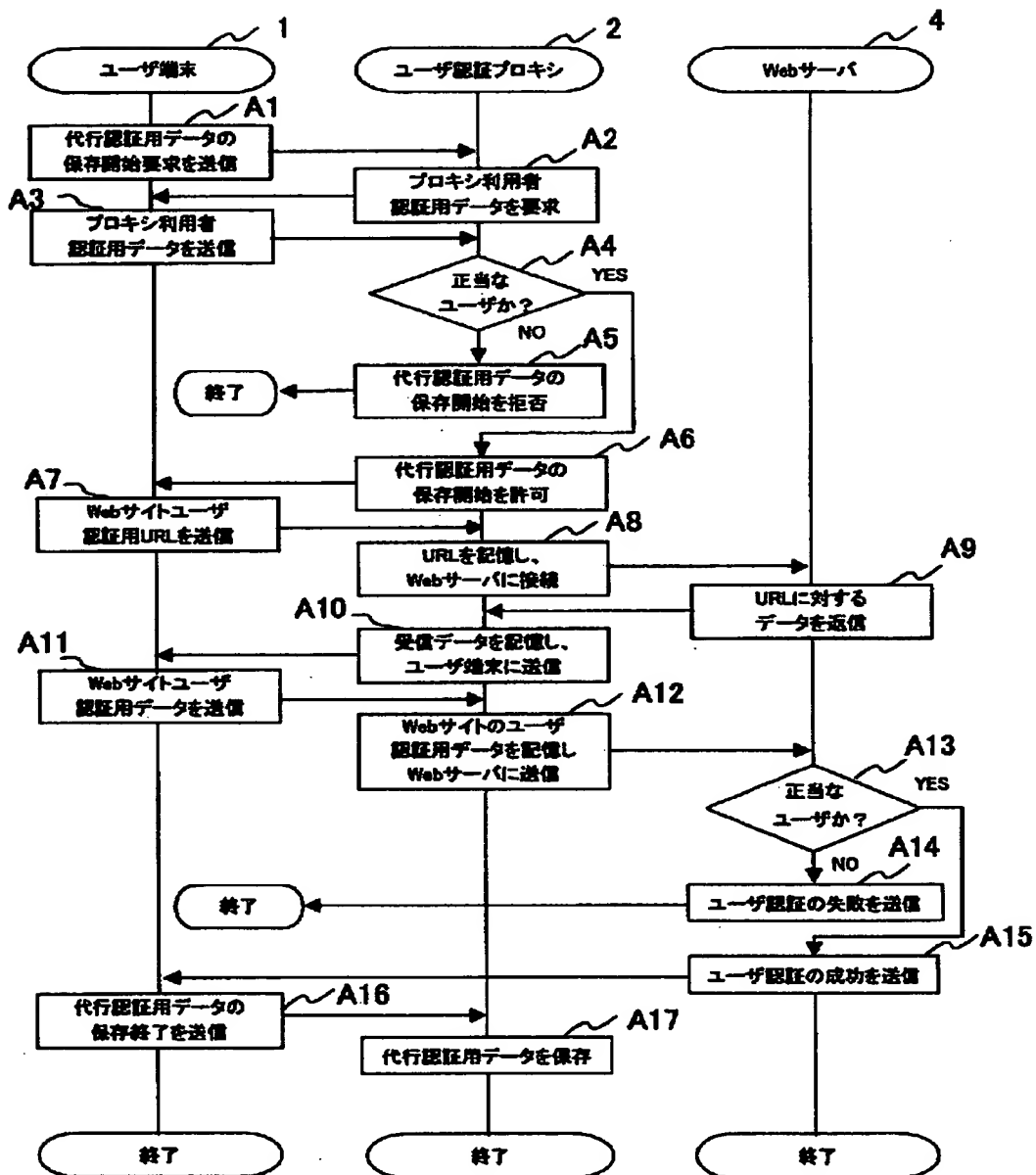
【図1】



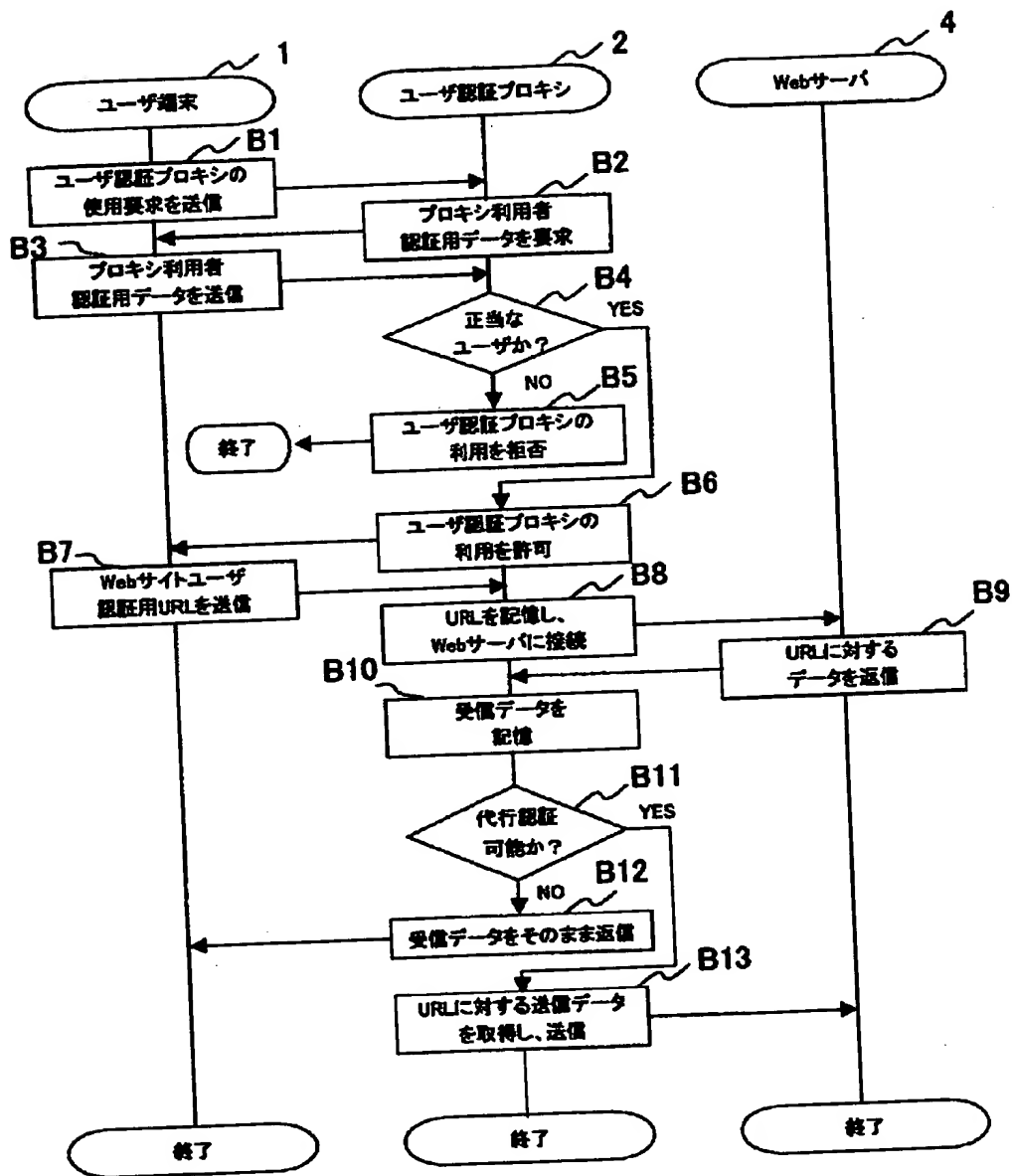
【図2】



【図3】



【図4】



【図5】

ユーザID	パスワード
00001	pKi#1_*)
00002	sE=CS(&1
...	...

【図6】

ユーザID	URL	受信データ	送信データ
00001	http://www.ncc.co.jp/customer.html	受信データ1	送信データ1
00001	http://www.shop1.co.jp/buyer.html	受信データ2	送信データ2
00002	http://www.ncc.co.jp/customer.html	受信データ3	送信データ3
00002	http://www.books.co.jp/buyer.html	受信データ4	送信データ4
...

【図7】

受信データ1

```
<HTML>
<BODY>
<FORM ACTION="/cgi-bin/mem_chk" METHOD="POST">
<table>
<tr><td>User ID</td><td><input type="text" name="uid"></td></tr>
<tr><td>Password</td><td><input type="password" name="pwd"></td></tr>
<tr><td><input type="submit" value="Submit"></td></tr>
</table>
</FORM>
</BODY>
</HTML>
```

送信データ1

```
uid=00001&pwd=nfi1ce_9
```

【図8】

受信データ2

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="member.xsl"?>
<member>
  <user_id></user_id>
  <password></password>
</member>
```

送信データ2

```
<?xml version="1.0"?>
<?xml-stylesheet type="text/xsl" href="member.xsl"?>
<member>
  <user_id>00001</user_id>
  <password>nfi1ce_9</password>
</member>
```

【書類名】 要約書

【要約】

【課題】

ユーザ認証を必要とする任意のWebサイトに対して、ユーザ認証を代行することで、ユーザの負担を軽減するシステム及び方法の提供。

【解決手段】

ユーザ端末1とWebサーバ4との間に設けられたユーザ認証プロキシ2が、ユーザがユーザ端末を利用してWebサーバとの間で行った一連のユーザ認証プロセスに係わる情報としてWebサイトのURL、ユーザ認証用にユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用にユーザ端末がWebサーバへ送信したユーザ認証用データを保存し、ユーザが任意のユーザ端末を利用してWebサイトのURLを指定した場合、該URLで指示されるWebサーバから該URLに対するデータを受信した際に受信データと保存されている受信データを比較し、等しい場合にWebサーバからの受信データをユーザ端末に転送せず、保存されているユーザ認証用の送信データをユーザ端末に代わってWebサーバに送信する。

【選択図】

図1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 2 3 7]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社